United Nations A/55/140/Add.1

General Assembly

Distr.: General
3 October 2000

Original: English

Fifty-fifth session
Agenda item 68
Developments in the field of information and telecommunications in the context of international security

Developments in the field of information and telecommunications in the context of international security

Report of the Secretary-General

Addendum

Contents

	Page
Replies received from Governments	2
Poland	2

00-67080 (E) 051000

Replies received from Governments

Poland

[Original: English]
[8 September 2000]

General appreciation of the issues of information security and definition of basic notions

1. information and telecommunications technology facilities substantially the free flow of information and brings enormous benefits to individuals, businesses and Governments worldwide. It enhances the development of democracy and freedom of speech as well as the advancement of a civil society. Poland believes it is important to promote and ensure further development in the field of information and telecommunications technology, along with the reinforcement of the principle of freedom of information and of choice and use of its technical conveyor.

2. Poland recognizes that there exists a potential threat of unauthorized interference with or misuse of information and telecommunications systems, the integrity of information-based critical infrastructures and the information resources of individuals, enterprises, educational or medical institutions and other private sector organizations, as well as of Governments. Information security embracing a wide range of issues related to the security of information and telecommunications systems necessitates the protection of accessibility, confidentiality, availability and integrity of the information processed in these systems. Information security also extends to the protection of information related to military capabilities and other aspects of national security. Insufficient protection of information resources and information and telecommunications systems that are vital from the point of view of the interests of the States concerned may also pose a threat to international security.

3. Poland believes, however, that existing risks are transboundary in character and that the technologies enabling attacks on information and telecommunications systems are widely available to all. At the same time, they cannot be classified as inherently civil or military in nature. Those threats derive mainly from criminal misuse by individuals or terrorist organizations and as such cannot be contained by traditional arms control agreements as they could restrict or inhibit the free flow of information and the peaceful uses of information technology, upon which all economies worldwide depend. Any preventive action aimed at containing potential criminal or terrorist attacks, including a danger to international peace, should focus on the protection of information resources and information-based systems.

4. To protect the integrity of information-based critical infrastructures and information resources in order to counteract risks to information security, Poland supports efficient and comprehensive international legal cooperation, as well as strict implementation of existing domestic legislation and the development of new legislation where necessary.

Domestic action

5. Every country has both the right and the responsibility to protect its own information and information-based systems. To this end, Poland has developed legal regulations as follows:

(a) The Law on the protection of classified information of 22 January 1999 which determines the rules for the mentioned protection;

(b) The Law on the protection of personal data of 29 October 1997, which regulates rules of conduct for data-processing as well as the rights of the individuals whose data are processed;

(c) The Penal Code of 6 June 1997, which establishes a penal responsibility not only for traditional types of crimes against the protection of information — namely disclosure of classified and restricted information — but also against destruction or removal of the data recorded on a computer, or damage or changes thereto, and against interference with or making impossible automatic accumulation or transmission of information relating to national defence, security of communication and the administrative functioning of government.

Advisability of developing international principles and action

6. Tremendous progress in information and telecommunications technology requires the development of international law in order to enhance information security. The issue of information criminality, including legal aspects, were among the main subjects of the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, held from 10 to 17 April 2000 (see A/CONF.187/15), and Poland recognizes the leading role of the United Nations Commission on Crime Prevention and Criminal Justice in developing international principles of information security and elaborating possible methods and means of action which would respect the necessity of a balance between the right of an individual to privacy and the duties of the various branches of government. This forum also facilitates and helps to coordinate the activities of the interregional and regional institutions on the prevention of crime and the treatment of offenders.

7. At the same time, Poland has been actively developing strong intergovernmental cooperation (with Germany – agreement concluded with Estonia, France, Hungary, Slovakia and Ukraine — negotiations under way) to conclude agreements concerning the protection of information, such as personal data, data relating to medical examinations, intellectual property rights or the outcome of scientific research against any unauthorized interference or any other crime, including forgery, illegal banking or financial transactions, and the protection of information resources and networks against deliberate damage.